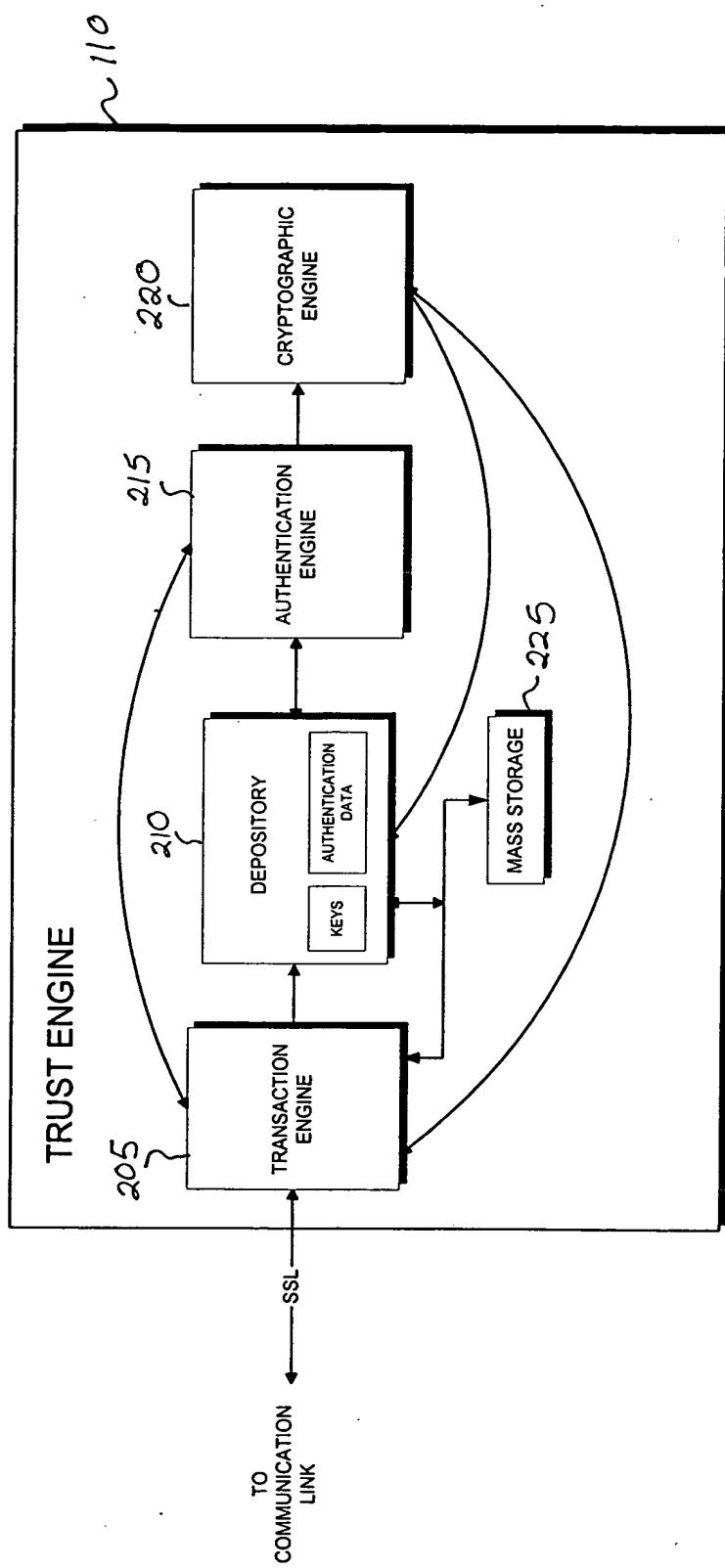


FIG. 1

FIG. 2



000260 248960

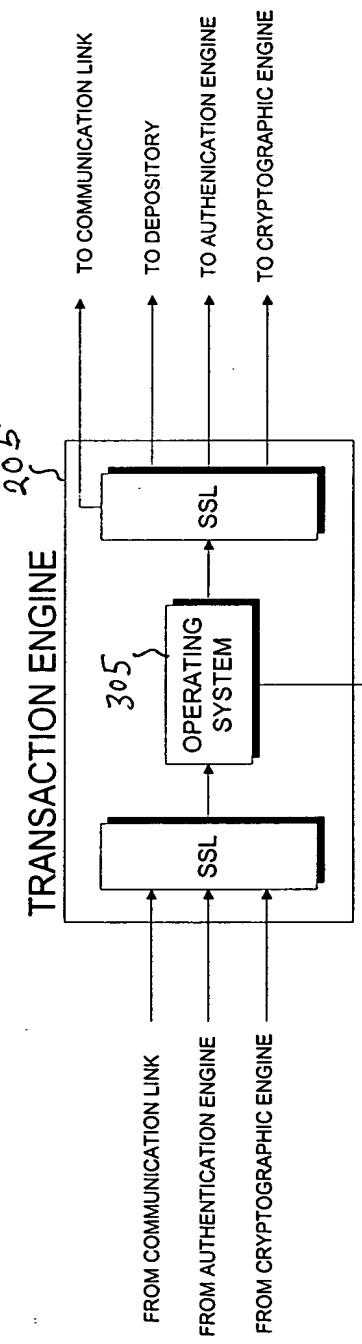


FIG. 3

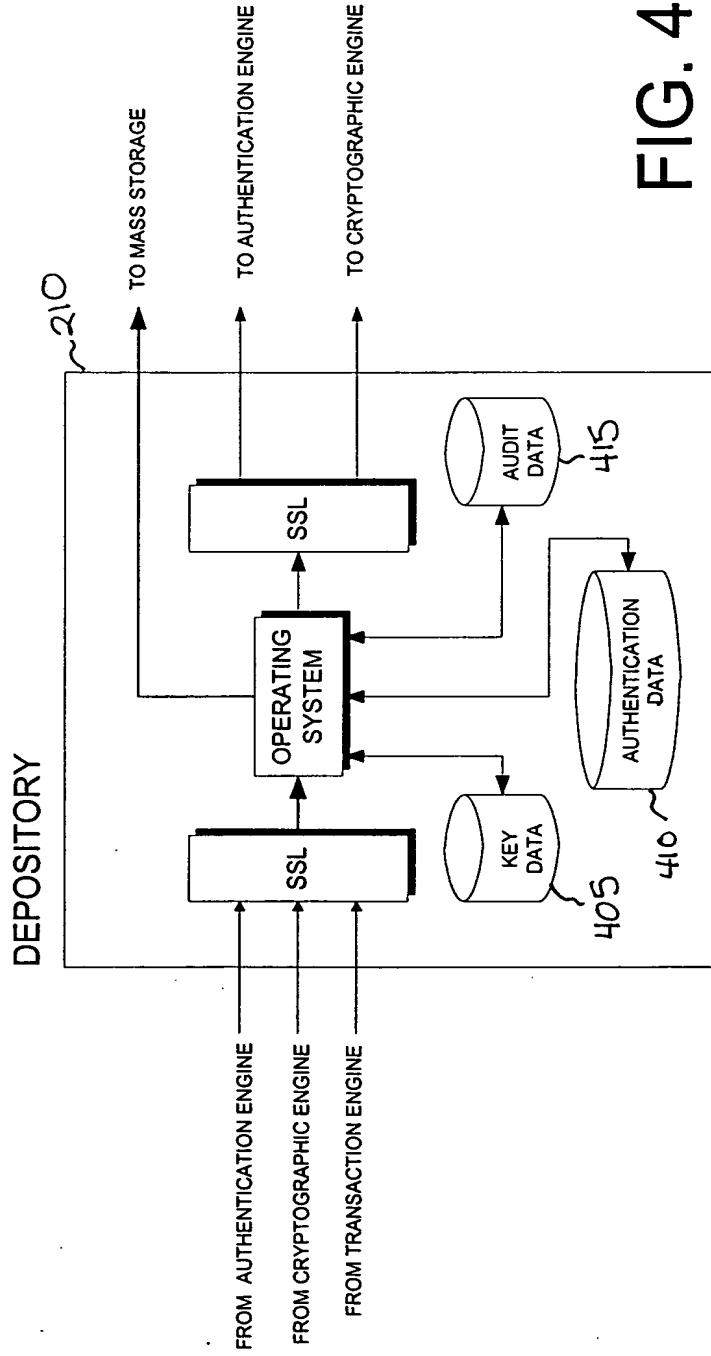


FIG. 4

AUTHENTICATION ENGINE

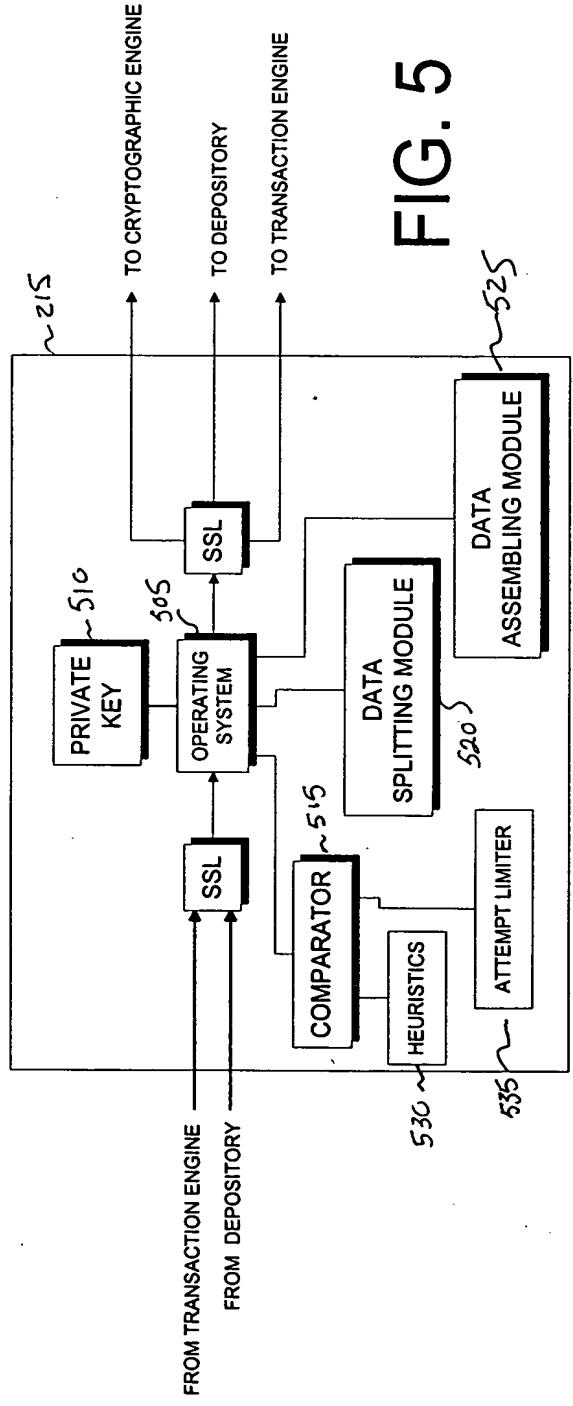


FIG. 5

CRYPTOGRAPHIC ENGINE

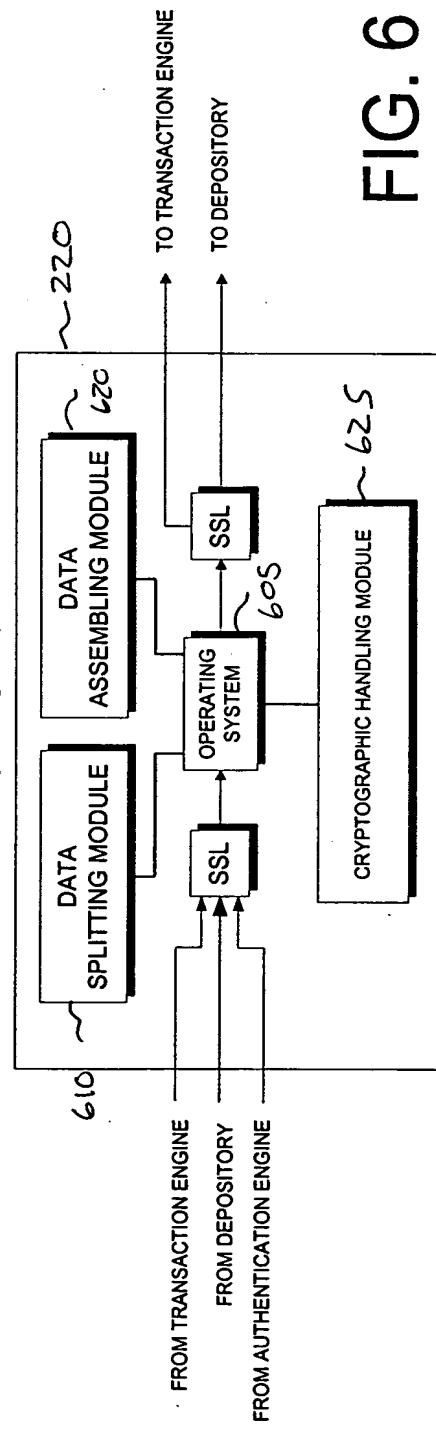


FIG. 6

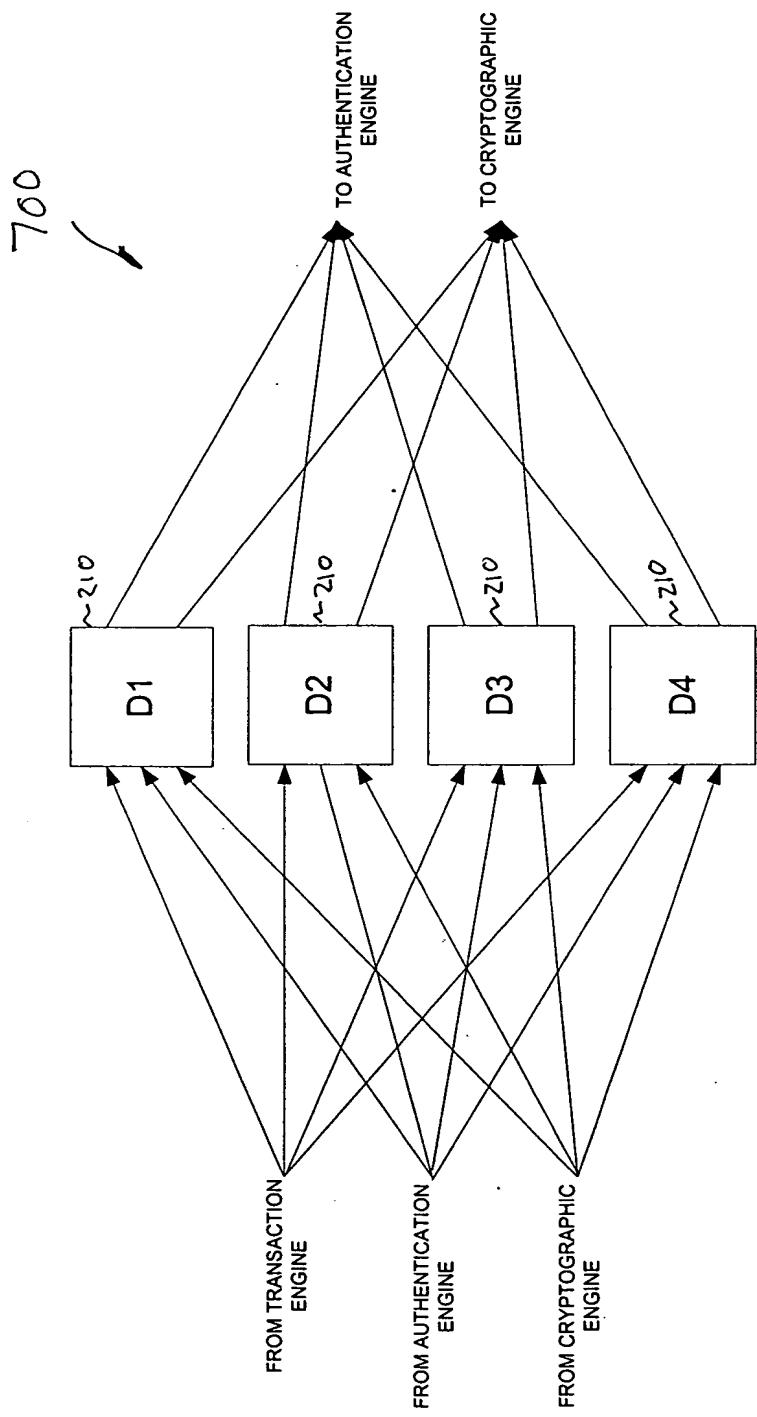


FIG. 7

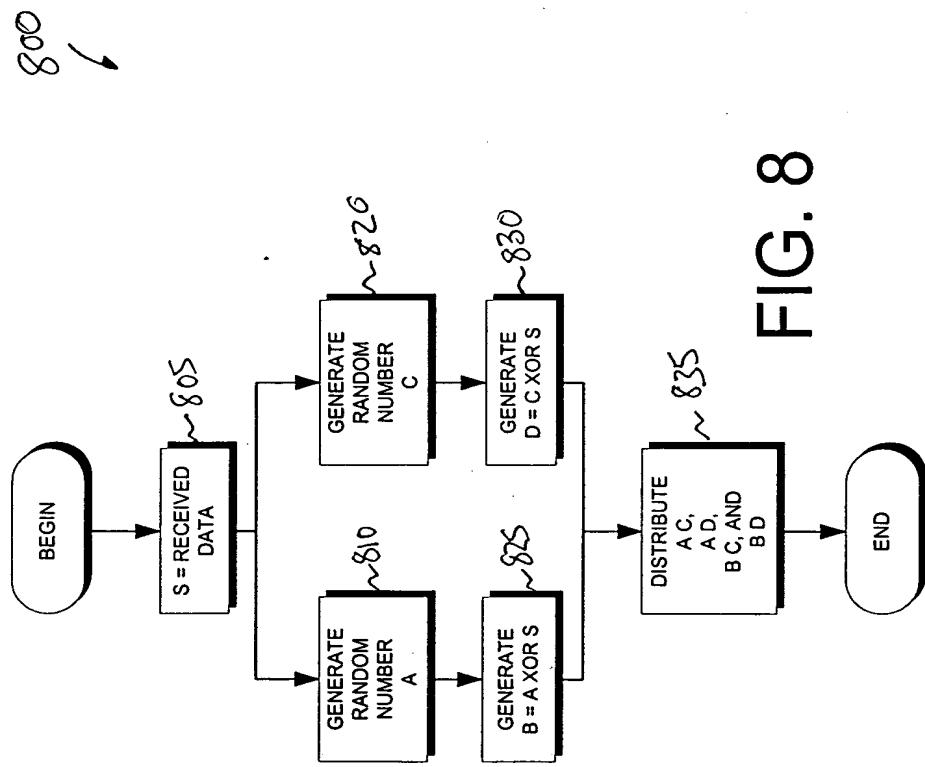


FIG. 8

900



ENROLLMENT DATA FLOW			
SEND	RECEIVE	SSL	ACTION
905 ~ USER	TRANSACTION ENGINE (TE)	½	TRANSMIT ENROLLMENT AUTHENTICATION DATA (B) AND THE USER ID (UID) ENCRYPTED WITH THE PUBLIC KEY OF THE AUTHENTICATION ENGINE (AE) AS (PUB_AE(UID, B))
915 ~ TE	AE	FULL	FORWARD TRANSMISSION
920 ~			AE DECRYPTS AND SPLITS FORWARDED DATA
925 ~ AE	THE X TH DEPOSITORY (DX)	FULL	STORE RESPECTIVE PORTION OF DATA
WHEN DIGITAL CERTIFICATE REQUESTED			
930 ~ AE	CRYPTOGRAPHIC ENGINE (CE)	FULL	REQUEST KEY GENERATION
935 ~			CE GENERATES AND SPLITS KEY
945 ~ CE	TE	FULL	TRANSMIT REQUEST FOR DIGITAL CERTIFICATE
950 ~ TE	CERTIFICATION AUTHORITY (CA)	½	TRANSMIT REQUEST
955 ~ CA	TE	½	TRANSMIT DIGITAL CERTIFICATE
960 ~ TE	USER	½	TRANSMIT DIGITAL CERTIFICATE
965 ~ TE	MS	FULL	STORE DIGITAL CERTIFICATE
	DX	FULL	STORE RESPECTIVE PORTION OF KEY

FIG. 9A

00666372 - 002000

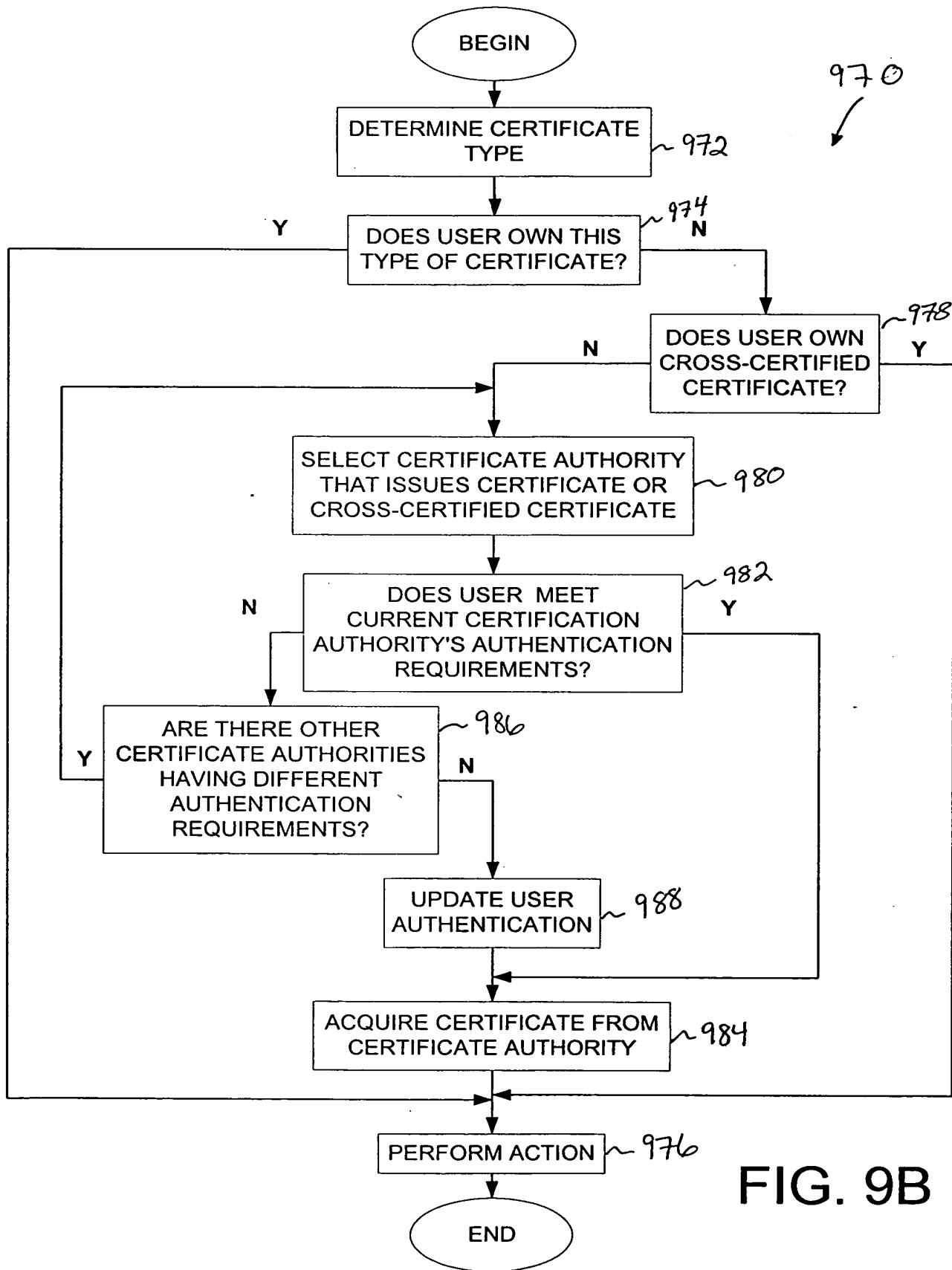


FIG. 9B

1000

AUTHENTICATION DATA FLOW				
	SEND	RECEIVE	SSL	ACTION
1005 ~	USER	VENDOR	½	TRANSACTION OCCURS, SUCH AS SELECTING PURCHASE
1010 ~	VENDOR	USER	½	TRANSMIT TRANSACTION ID (TID), AND AUTHENTICATION REQUEST (AR)
0105 ~				AUTHENTICATION DATA (B') IS GATHERED FROM USER
0120 ~	USER	TE	½	TRANSMIT TID AND B' WRAPPED IN THE PUBLIC KEY OF THE AUTHENTICATION ENGINE (AE), AS (PUB_AE(TID, B'))
0125 ~	TE	AE	FULL	FORWARD TRANSMISSION
0130 ~				ENROLLMENT AUTHENTICATION DATA (B) IS REQUESTED AND GATHERED
0135 ~	VENDOR	TRANSACTION ENGINE (TE)	FULL	TRANSMITS TID, AR
0140 ~	TE	MASS STORAGE (MS)	FULL	CREATE RECORD IN DATABASE
0145 ~	TE	THE X TH DEPOSITORY (DX)	FULL	UID, TID
0150 ~	DX	AE	FULL	TRANSMIT THE TID AND THE PORTION OF THE AUTHENTICATION DATA STORED AT ENROLLMENT (BX) AS (PUB_AE(TID, BX))
0155 ~				AE ASSEMBLES B AND COMPARES TO B'
	AE	TE	FULL	TID, THE FILLED IN AR
	TE	VENDOR	FULL	TID, YES/NO
	TE	USER	½	TID, CONFIRMATION MESSAGE

FIG. 10

1100

SIGNING DATA FLOW			
SEND	RECEIVE	SSL	ACTION
USER	VENDOR	½	TRANSACTION OCCURS, SUCH AS AGREEING ON A DEAL
VENDOR	USER	½	TRANSMIT TRANSACTION IDENTIFICATION NUMBER (TID), AUTHENTICATION REQUEST (AR), AND AGREEMENT OR MESSAGE (M)
			CURRENT AUTHENTICATION DATA (B') AND A HASH OF THE MESSAGE RECEIVED BY THE USER ($h(M')$) IS GATHERED FROM USER
USER	TE	½	TRANSMIT TID, B', AR, AND $h(M')$ WRAPPED IN THE PUBLIC KEY OF THE AUTHENTICATION ENGINE (AE) AS ($PUB_AE(TID, B', h(M'))$)
TE	AE	FULL	FORWARD TRANSMISSION
			GATHER ENROLLMENT AUTHENTICATION DATA
VENDOR	TRANSACTION ENGINE (TE)	FULL	TRANSMITS UID, TID, AR, AND A HASH OF THE MESSAGE ($h(M)$).
TE	MASS STORAGE (MS)	FULL	CREATE RECORD IN DATABASE
TE	THE X TH DEPOSITORY (DX)	FULL	UID, TID
DX	AE	FULL	TRANSMIT THE TID AND THE PORTION OF THE AUTHENTICATION DATA STORED AT ENROLLMENT (BX) AS ($PUB_AE(TID, BX)$)
			THE ORIGINAL VENDOR MESSAGE IS TRANSMITTED TO THE AE
TE	AE	FULL	TRANSMIT $h(M)$
			AE ASSEMBLES B, COMPARES TO B' AND COMPARES $h(M)$ TO $h(M')$
105~	AE	CRYPTOGRAPHIC ENGINE (CE)	REQUEST FOR DIGITAL SIGNATURE AND A MESSAGE TO BE SIGNED, FOR EXAMPLE, THE HASHED MESSAGE
110~	AE	DX	TID, SIGNING UID
115~	DX	CE	TRANSMIT THE PORTION OF THE CRYPTOGRAPHIC KEY CORRESPONDING TO THE SIGNING PARTY
120~			CE ASSEMBLES KEY AND SIGNS
125~	CE	AE	TRANSMIT THE DIGITAL SIGNATURE (S) OF SIGNING PARTY
130~	AE	TE	TID, THE FILLED IN AR, $h(M)$, AND S
135~	TE	VENDOR	TID, A RECEIPT = (TID, YES/NO, AND S), AND THE DIGITAL SIGNATURE OF THE TRUSTENGINE, FOR EXAMPLE, A HASH OF THE RECEIPT ENCRYPTED WITH THE TRUSTENGINE'S PRIVATE KEY ($Priv_TE(h(RECEIPT)$)
140~	TE	USER	½ TID, CONFIRMATION MESSAGE

FIG. 11

1200

ENCRYPTION/DECRYPTION DATA FLOW				
SEND	RECEIVE	SSL	ACTION	
DECRYPTION				
			PERFORM AUTHENTICATION DATA PROCESS 1000, INCLUDE THE SESSION KEY (SYNC) IN THE AR, WHERE THE SYNC HAS BEEN ENCRYPTED WITH THE PUBLIC KEY OF THE USER AS PUB_USER(SYNC)	
			AUTHENTICATE THE USER	
1205 ~	AE	CE	FULL	FORWARD PUB_USER(SYNC) TO CE
1210 ~	AE	DX	FULL	UID, TID
1215 ~	DX	CE	FULL	TRANSMIT THE TID AND THE PORTION OF THE PRIVATE KEY AS (PUB_AE(TID, KEY_USER))
1220 ~				CE ASSEMBLES THE CRYPTOGRAPHIC KEY AND DECRYPTS THE SYNC
1225 ~	CE	AE	FULL	TID, THE FILLED IN AR INCLUDING DECRYPTED SYNC
1230 ~	AE	TE	FULL	FORWARD TO TE
	TE	REQUESTING APP/VENDOR	½	TID, YES/NO, SYNC
ENCRYPTION				
1235 ~	REQUESTING APP/VENDOR	TE	½	REQUEST FOR PUBLIC KEY OF USER
1240 ~	TE	MS	FULL	REQUEST DIGITAL CERTIFICATE
1245 ~	MS	TE	FULL	TRANSMIT DIGITAL CERTIFICATE
1250 ~	TE	REQUESTING APP/VENDOR	½	TRANSMIT DIGITAL CERTIFICATE

FIG. 12

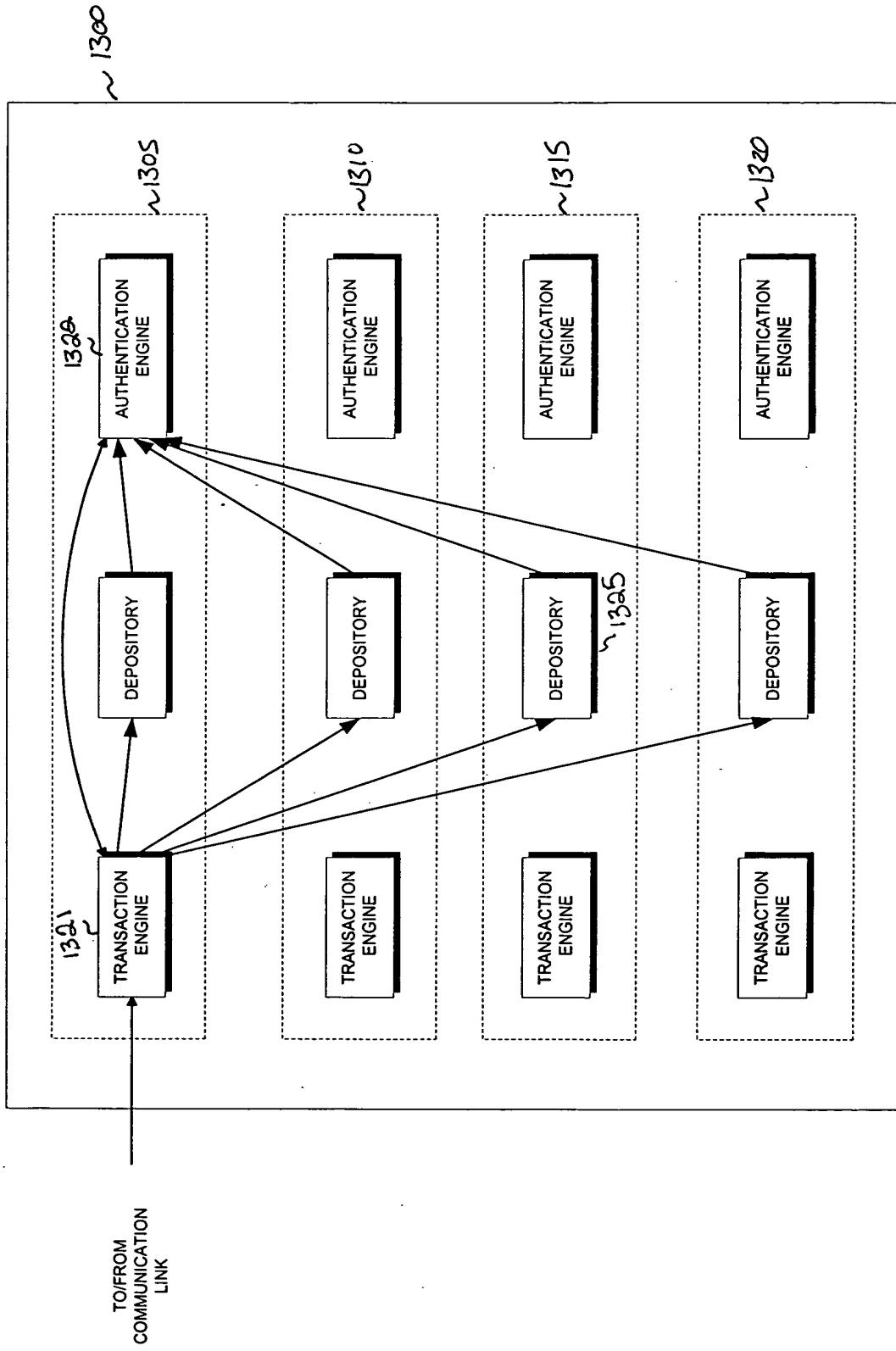


FIG. 13

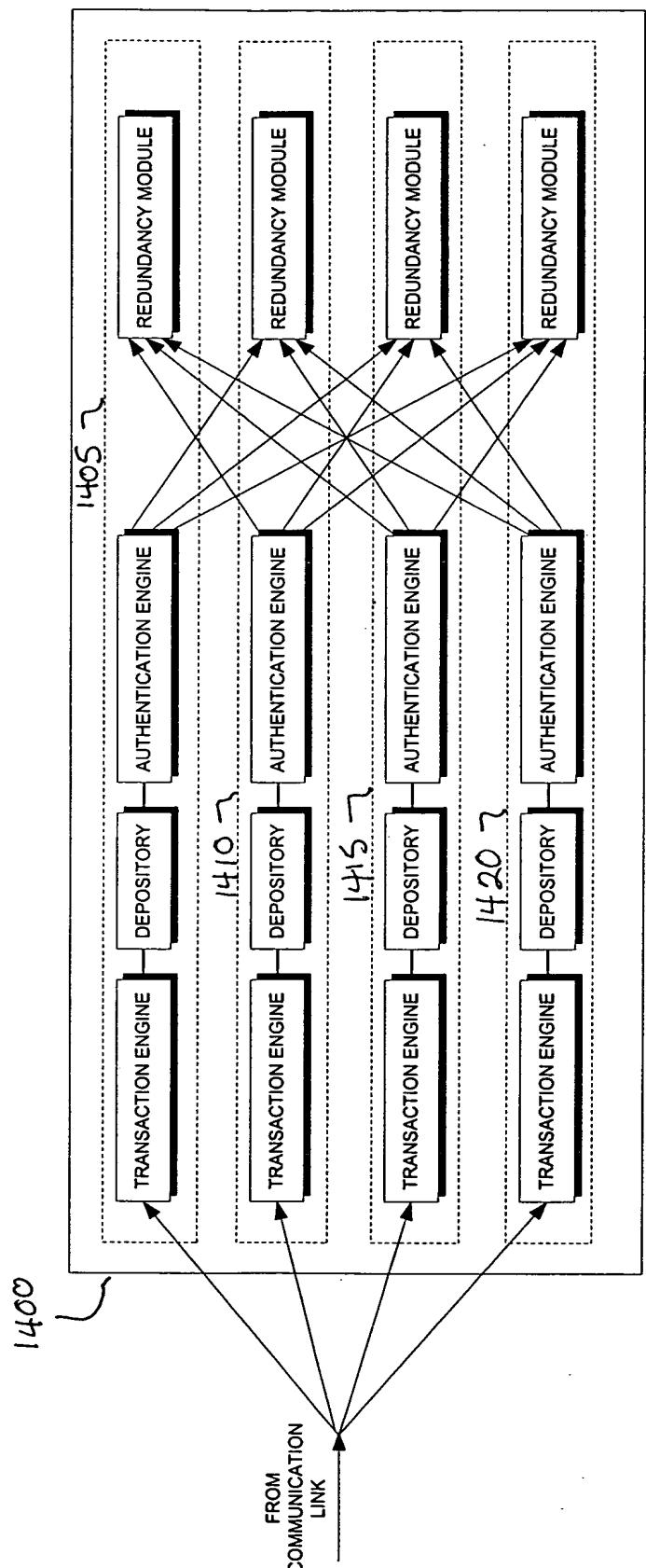


FIG. 14

FIG. 15

REDUNDANCY MODULE



FIGURE 16

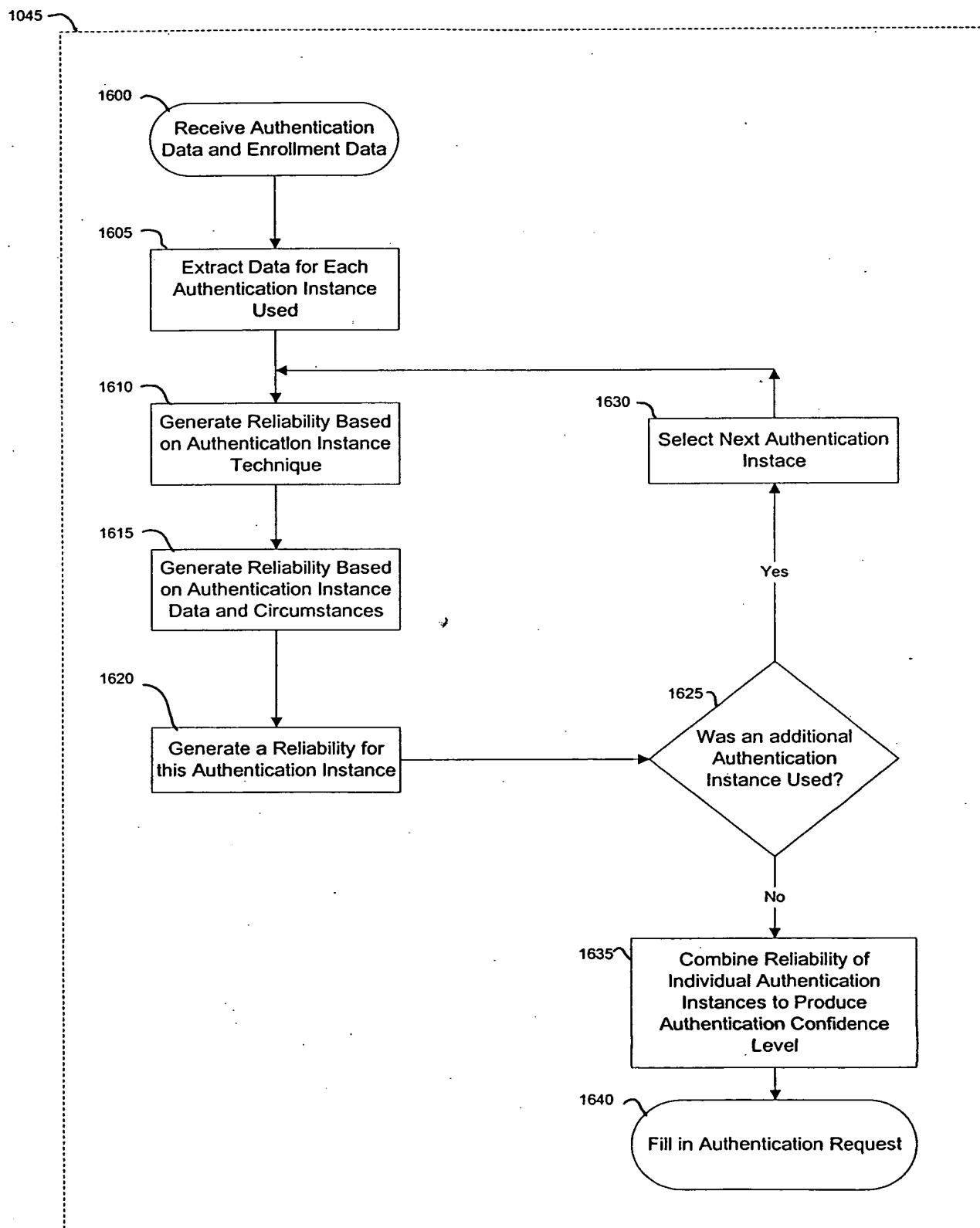


FIGURE 17

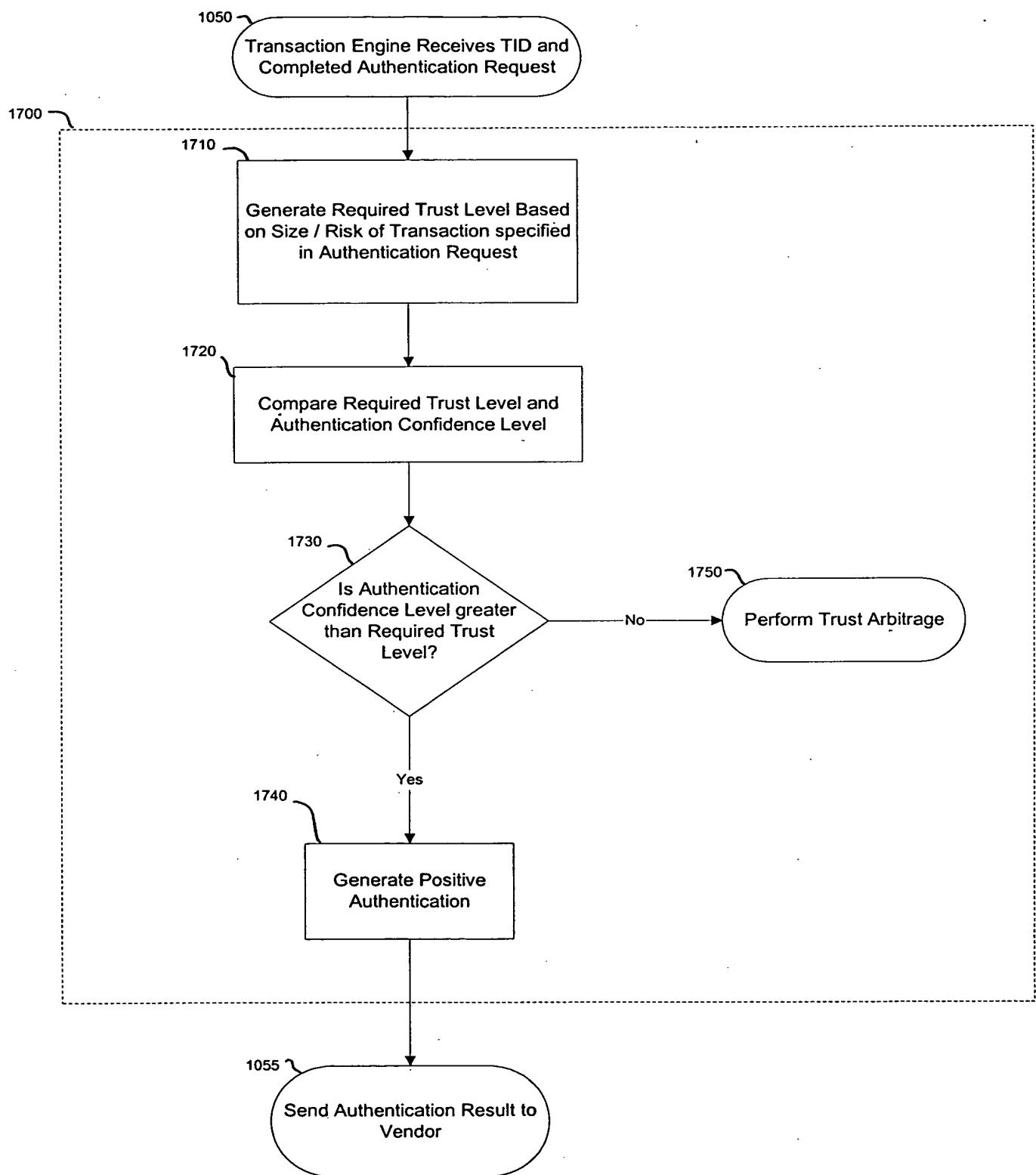


FIGURE 18

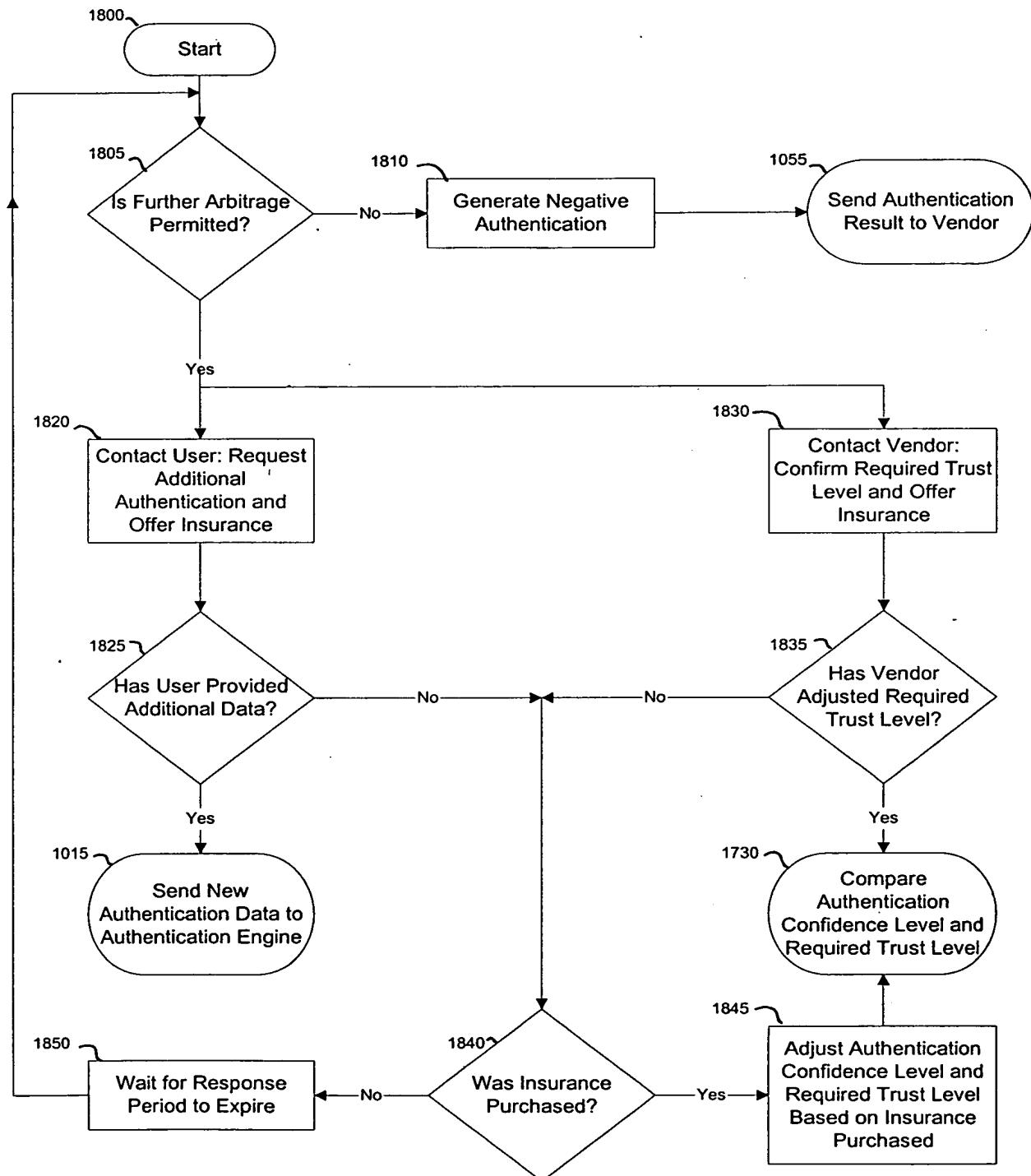


FIGURE 19

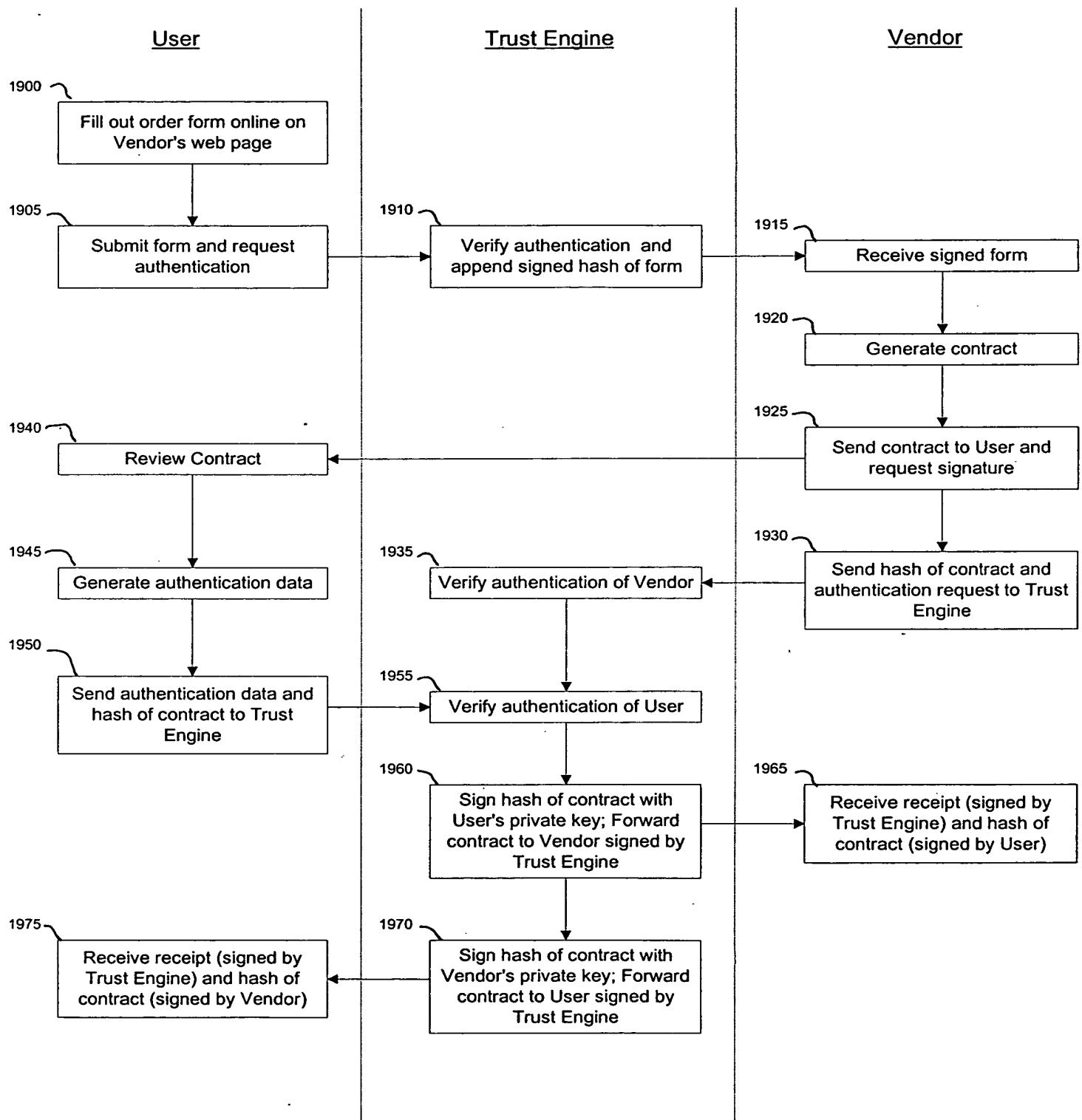


FIGURE 20

